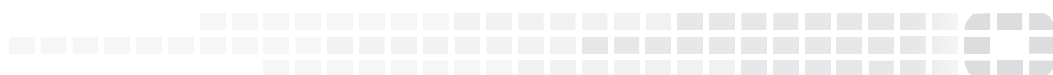




FORTINET

High Performance Network Security



FortiMail™ Release Notes

VERSION 5.4.5 GA



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



March 29, 2018

TABLE OF CONTENTS

Introduction	4
Supported Platforms	4
What's New	5
Special Notices	6
TFTP firmware install.....	6
Monitor settings for web UI	6
Recommended browsers on desktop computers for administration and Webmail.....	6
Recommended browsers on mobile devices for Webmail access	6
FortiSandbox support	6
Firmware Upgrade/Downgrade.....	7
Before and after any firmware upgrade/downgrade	7
Upgrade path	7
For any 5.x release	7
For any 4.x release	7
Firmware downgrade.....	8
Downgrading from 5.4.5 to 5.x or 4.x releases.....	8
Resolved Issues	9
Antivirus/Antispam/Content	9
Mail Receiving and Delivering.....	9
System	9
Log and Report.....	10
Admin GUI/Webmail	10
Known Issues	11
Image Checksums	12

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 5.4.5 release, build 0719.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

The following table summarizes the new features and enhancements in this release.

Features	Descriptions
DLP scanning	Added DLP sensitive data scanning option to Subject content when defining a DLP rule.
Toggle On/Off selected quarantine entries	Under Monitor > Quarantine, after CTRL-selecting multiple entries for bulk releasing or deleting, you can now deselect an item by CTRL-select the item.
WCCP support	Support WCCP using 2 or more FortiMail units as clients.
HTTP security header	Two headers (Content-Security-Policy and X-Content-Type-Options) have been added to admin GUI and webmail GUI HTTP response headers.

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 and Edge 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 10, 11
- Official Google Chrome browser for Android 6.0 to 8.0

FortiSandbox support

- FortiSandbox 2.3 and above

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, challenge/response should be used.

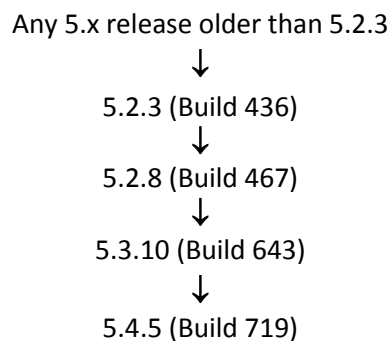
Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

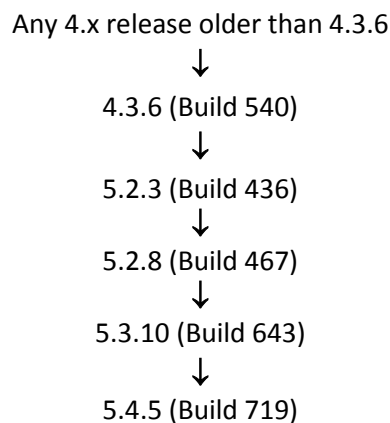
- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System > Maintenance > Configuration*.
- After any firmware upgrade/downgrade:
 - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
 - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

Upgrade path

For any 5.x release



For any 4.x release



After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard > Status* on the Web UI.

Firmware downgrade

Downgrading from 5.4.5 to 5.x or 4.x releases

Downgrading from 5.4.5 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.4.5 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Antivirus/Antispam/Content

Bug ID	Description
477064	Some rescan email is released before FortiSandbox verdict.
471131	Recipient outbound policies with protected domain as sender pattern are not triggered when email is sent from webmail.
477659	DKIM signatures are inserted twice if the outbound email is inspected by FortiSandbox.
474861	HTML content is not converted to text even though this feature is enabled in the content profile.
447735	Part of email body is lost after converting HTML to text by the content profile.
479590	Email attachment file size is calculated incorrectly.

Mail Receiving and Delivering

Bug ID	Description
474266	Email is sent to a server defined in a routing profile after a few delivery tries.
477351	Cannot reach the relay host using FQDN.
470130	IBE encryption using Access Control Delivery rules always matches wildcard domains instead of more specific recipients.
474627	When disclaimer is inserted, some incoming email body is displayed as attachment in Outlook.

System

Bug ID	Description
478702	The mailfilterd process causes high CPU usage.
475741	Mail migration appends symbols to IMAP passwords.
471556	Additional HTML tags are inserted in disclaimers.
476356	RADIUS users cannot be imported by using CSV files.
475724	After upgrading to 5.4.4 release, the CPU usages reaches 100%.
475337	Admin profile changes are not synchronized to the HA slave unit.
475348	FortiGuard antispam override IP address is not used if it is a public address.
475042	Session profile advanced mail routing to MX record of alternative domain does not work.

Bug ID	Description
409777	Some system events SNMP traps are not sent.
475078	
469618	
469984	After upgrading from 5.4.2 to 5.4.4, the rotated quarantine folders cannot be opened.
473488	In some cases, the system quarantine messages cannot be released.
473696	Cannot create SNMPv3 users under System > Configuration > SNMP.
472457	Internal Server Error occurs when downloading PKCS12 file of certification which status is pending.
480712	When the email archive account disk quota is full, the previously rotated folders will be deleted.

Log and Report

Bug ID	Description
469409	CRLF is not displayed properly by SPF check in logs.
475040	In some cases, report generation may stop when Daylight Saving Time starts.
475545	Non-US-ASCII logs sent to FortiAnalyzer are not searchable.

Admin GUI/Webmail

Bug ID	Description
477852	With Internet Explorer and Edge, the empty Calendar Resource table is not displayed properly in webmail.
477882	The Compose button is missing for internal IBE users in webmail.
472978	Cyrillic characters are not displayed properly in quarantine preview.
473566	When FortiMail VM cannot access the Internet, a meaningless message is displayed.
472967	Under System > Maintenance > Mail Data > Backup Options, the "Initiator name as username" option should not appear when iSCSI Server is not selected.
474405	Under Security > Bayesian > Domain, the Bayesian database cannot be restored.
472469	Bridge should not be selectable on virtual IP action of HA configuration when the operation mode is server or gateway.
470864	Japanese translation of "Instant Message" is wrong on the View/Edit Contact page in webmail.
469367	Japanese translation of AOL Instant Messenger (AIM) is wrong on the View/Edit Contact page in webmail.
469887	Russian characters for system_spam resource key may cause the webmail inaccessible.

Known Issues

The following table lists some minor known issues. .

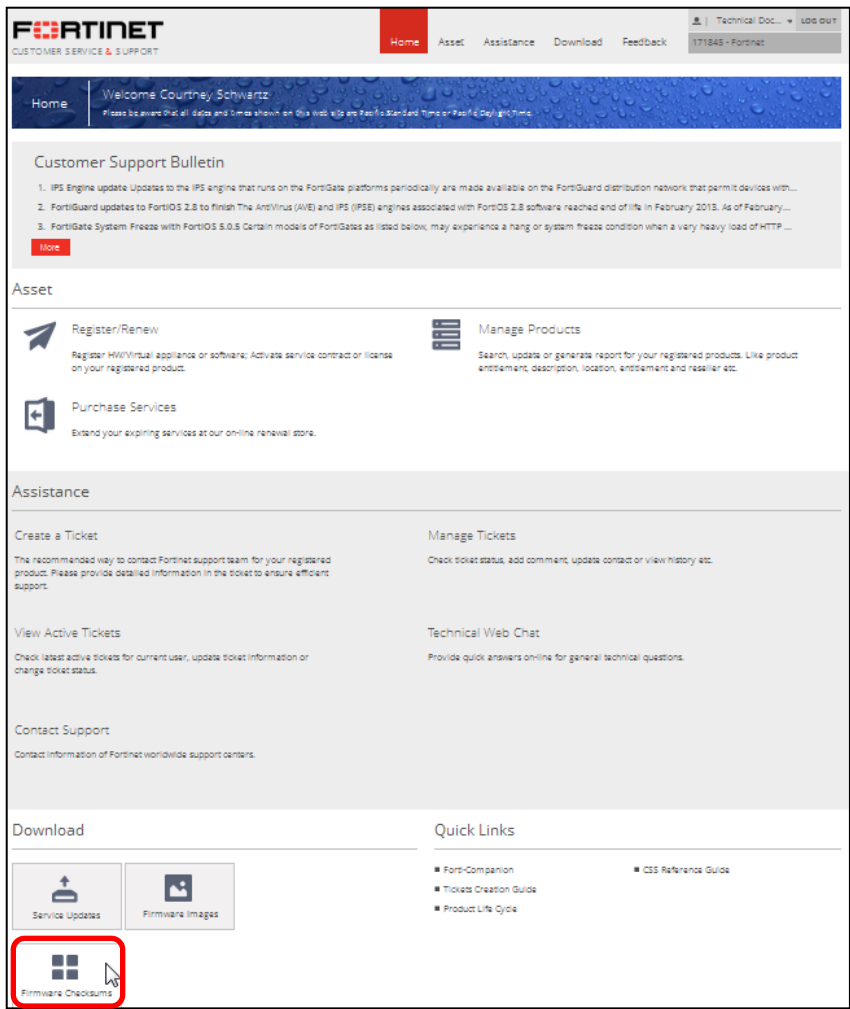
Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

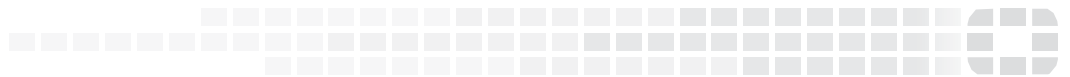
MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool





High Performance Network Security



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.